Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) MARTINO	Membro designato dalla Banca d'Italia
(BO) DI STASO	Membro designato dalla Banca d'Italia
(BO) SOLDATI	Membro di designazione rappresentativa degli intermediari
(BO) PETRAZZINI	Membro di designazione rappresentativa dei clienti

Relatore BARBARA PETRAZZINI

Seduta del 15/02/2022

Esame del ricorso n. 1380426/2021 del 30/09/2021

proposto da XXXXXXX

nei confronti di 1030 - BANCA MONTE PASCHI SIENA

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) MARTINO	Membro designato dalla Banca d'Italia
(BO) DI STASO	Membro designato dalla Banca d'Italia
(BO) SOLDATI	Membro di designazione rappresentativa degli intermediari
(BO) PETRAZZINI	Membro di designazione rappresentativa dei clienti

Relatore BARBARA PETRAZZINI

Seduta del 15/02/2022

FATTO

Con ricorso depositato in data 30 settembre 2021 parte ricorrente espone che:

- è titolare della carta di credito n. **095 emessa dall'intermediario odierno resistente;

- in data 3 aprile 2021, alle ore 11:33, riceveva un sms da parte dell'intermediario che la avvisava che un dispositivo non autorizzato risultava connesso al suo conto corrente e che per disconoscere l'operazione doveva cliccare sul link ivi contenuto;

- ella non faceva alcunché, ma alle 12:35 veniva contattata sul cellulare da un dipendente dell'ufficio frodi dell'intermediario che la informava che ignoti avevano tentato di accedere al suo conto;

- seguiva dunque le istruzioni dell'operatore che le diceva di inserire i codici che le giungevano sul proprio cellulare al fine di bloccare le operazioni sospette;

- poco dopo scopriva che erano state effettuate due operazioni con la propria carta di credito per un totale di 1.172,73 euro;

- il giorno stesso sporgeva denuncia e inoltrava reclamo all'intermediario.

A fronte di negativo riscontro da parte dell'intermediario, si rivolge pertanto a quest'Arbitro chiedendo la restituzione dell'importo complessivo di 1.172,73 euro corrispondente

all'importo delle operazioni fraudolentemente eseguite.

Costituendosi nel procedimento l'intermediario resistente eccepisce che:

- le verifiche effettuate hanno portato al rifiuto della richiesta di rimborso poiché le operazioni in questione sono state eseguite con le informazioni riferite dalla ricorrente, come affermato dalla stessa;

- le operazioni, pertanto, sono state correttamente registrate, contabilizzate e concluse con l'utilizzo della carta originale e del relativo codice otp ricevuto dalla ricorrente;

- la ricorrente, rivelando al truffatore i codici ricevuti tramite sms ha agevolato la realizzazione delle operazioni;

- la vicenda in esame rientra nei casi di c.d. smishing, fenomeno di tale diffusione che anche i Collegi ABF ritengono da tempo che l'impiego della normale diligenza sia sufficiente a scongiurare il pericolo e a impedire la truffa;

- la ricorrente è dunque incorsa in colpa grave (ex art. 12, d.lgs. 11/2010), caduta vittima di forme tradizionali di smishing;

- la banca ha posto in essere numerose campagne informative volte a informare la propria clientela al fine di prevenire le frodi;

- le operazioni sono andate a buon fine grazie al corretto inserimento delle credenziali statiche (numero della carta) e credenziali dinamiche (otp).

Conclude pertanto chiedendo il rigetto del ricorso.

Con successive memorie di replica, la ricorrente ribadisce la natura apparentemente genuina dell'sms ricevuto ed insiste nella richiesta di accoglimento della propria domanda; con proprie memorie, l'intermediario conferma quanto già esposto nelle controdeduzioni.

DIRITTO

La questione concerne la valutazione del comportamento della ricorrente e dell'intermediario resistente in relazione all'esecuzione, tramite un sistema di sicurezza a più fattori, di due operazioni di pagamento *on line* non autorizzate eseguite in data 3 aprile 2021 aventi ad oggetto la somma richiesta in restituzione di 1.172,735 euro.

La materia è disciplinata dal d.lgs. 11/2010 (emanato in attuazione della Direttiva 2007/64/CE e successivamente modificato dal d. lgs. 218/2017 in attuazione della Direttiva 2015/2366/UE). Dalla richiamata normativa e, in particolare, dall'art. 10 del d. lgs. 11/2010, discende che, qualora l'utilizzatore neghi -come nella vicenda oggetto del ricorso- di aver autorizzato un'operazione di pagamento eseguita, gravi sull'intermediario l'onere di provare l'avvenuta autenticazione della medesima operazione, la sua corretta registrazione e contabilizzazione, nonché il mancato verificarsi di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti. Tale prova –precisa il comma 2 del citato articolo- non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo

fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi sul medesimo gravanti, essendo onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente.

Nel caso di mancato assolvimento dell'onere probatorio di cui si è detto, l'intermediario è obbligato a riaccreditarne l'importo sul conto del cliente, ai sensi dell'art. 11 del medesimo d.lgs. n. 11/2010.

L'onere di dimostrare la colpa grave o il comportamento fraudolento del titolare dello strumento di pagamento grava quindi sull'intermediario, ma, come più volte affermato dai Collegi territoriali e dal Collegio di Coordinamento, la relativa prova può essere fornita mediante «indizi chiari, precisi e concordanti idonei a comprovare che la ricorrente non abbia custodito la carta di pagamento con la dovuta diligenza» (cfr. la decisione ABF, Collegio di coordinamento, n. 897/2014), ovvero, fermo restando che «la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio», essere fornita dall'intermediario indicando «una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente » (così la decisione ABF, Collegio di Coordinamento, n. 22745/2019).

Nel caso di specie, la ricorrente disconosce due operazioni dell'importo di 40,00 euro e di 1.132,73 euro avvenute alle ore 12:45 e 12:54 (rendendo nei fatti irrilevante, stante la breve distanza temporale tra le due transazioni, il presidio di sicurezza rappresentato dall'sms *alert*) e sostiene di essere rimasta vittima di una truffa informatica perpetrata tramite un artifizio che consente di alterare il mittente di un sms, facendo sì che il telefono cellulare lo "cataloghi" insieme a quelli, genuini, dell'intermediario; evidenzia, infatti, di aver ricevuto in data 3 aprile 2021 un sms apparentemente proveniente dall'intermediario, nel quale la si avvisava di un accesso al suo conto online da un dispositivo non riconosciuto e la si invitava a cliccare sul link contenuto nel messaggio; veniva quindi contattata telefonicamente da un sedicente operatore dell'intermediario che le forniva indicazioni utili a bloccare le operazioni sospette. Poco dopo si avvedeva che erano stati posti in essere due pagamenti online, dalla stessa disconosciuti.

A fronte delle contestazioni del ricorrente l'intermediario fornisce le tracciature informatiche relative alle operazioni, affermando che le stesse sono avvenute tramite un sistema di autenticazione forte, mediante inserimento dei dati della carta in possesso della titolare e di sua esclusiva conoscenza e corretto inserimento dei codici OTP inviati all'utenza telefonica della titolare della carta.

Osserva il Collegio che l'emittente ha l'obbligo di prevedere forme di autenticazione "forte" per l'autorizzazione di operazioni di pagamento a tutela della sicurezza delle operazioni stesse e del titolare del mezzo di pagamento.

La definizione di autenticazione forte si rinviene nell'art. 1, d.lgs. n. 11/2010, ove si prevede che per autenticazione forte del cliente si intende: «un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente) che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri (...)».

Occorre quindi verificare se nel caso in specie l'intermediario abbia fornito elementi a

sostegno della legittimità dell'operazione contestata. Sulla base delle dichiarazioni dell'intermediario, per effettuare ed autorizzare l'operazione disconosciuta sono stati richiesti i dati della carta e la password dinamica inviata al cellulare del ricorrente.

Secondo questo Collegio non sussistono, nel caso in questione, i presupposti per ritenere che un sistema di autenticazione forte sia stato attuato. Vale la pena ricordare che in base alle determinazioni dell'EBA (*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019) l'autenticazione forte del cliente «consiste in una procedura basata sull'impiego di due o più dei seguenti elementi - classificati nelle categorie della conoscenza, del possesso e dell'inerenza: i) qualcosa che solo l'utente conosce, per esempio una password statica, un codice, un numero di identificazione personale; ii) qualcosa che solo l'utente possiede, per esempio un token, una smart card, un cellulare; iii) qualcosa che caratterizza l'utente, per esempio una caratteristica biometrica, quale può essere un'impronta digitale. Inoltre, gli elementi selezionati devono essere reciprocamente indipendenti, ossia la violazione di un elemento non compromette l'altro o gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione».

Sempre secondo il parere dell'EBA, ai fini dell'autenticazione forte, i dati presenti sulla carta di pagamento non costituiscono elementi né di conoscenza, né di possesso. Diversamente ragionando si incorrerebbe in contraddizione con quanto previsto dall'art. 6 e 7 del Regolamento 389/2017, secondo cui gli elementi dell'autenticazione forte del cliente classificati come conoscenza e come possesso non devono essere catturabili o accessibili da soggetti terzi. Il numero della carta e il codice CCV, riportati in chiaro sul fronte e sul retro della carta, sono invece potenzialmente conoscibili e accessibili anche da parte di terzi. Ne deriva che l'unico fattore di autenticazione ad assumere rilievo nel caso di specie è l'invio dei codici OTP, utili ai fini della esecuzione delle operazioni contestate.

Poichè la data del 14 settembre 2019 costituisce il momento a decorrere dal quale trovano applicazione le nuove regole EBA in base alle quali non sono da ritenersi sufficienti come prova della corretta autenticazione "forte" i dati riportati sulla carta stessa, se questi sono uno dei due elementi richiesti per l'autenticazione stessa, ne consegue che, ad avviso di questo Collegio, l'intermediario odierno resistente non ha adottato, quantomeno nelle operazioni per cui è causa, gli standard di sicurezza corrispondenti alla disciplina oggi applicabile, nei termini sopra riassunti (negli stessi termini si vedano le decisioni ABF, Collegio di Bologna, n. 22586/2020, Collegio di Napoli, n. 17207/2020 e Collegio di Roma, n. 8493/2020).

La domanda della ricorrente merita pertanto accoglimento, con conseguente diritto alla restituzione dell'importo di 1.172,73 euro.

Il Collegio precisa infine che, trattandosi di ricorso presentato successivamente all'entrata in vigore delle nuove Disposizioni ABF, ai sensi di quanto previsto nella nota (3) di pag. 25 delle predette Disposizioni, l'importo finale contenuto nelle pronunce di accoglimento è arrotondato all'unità di euro (per eccesso se la prima cifra dopo la virgola è uguale o superiore a 5; per difetto, se la prima cifra dopo la virgola è inferiore a 5).

PER QUESTI MOTIVI

Il Collegio – in accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 1.173,00 (millecentosettantatre/00).

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARCELLO MARINARI